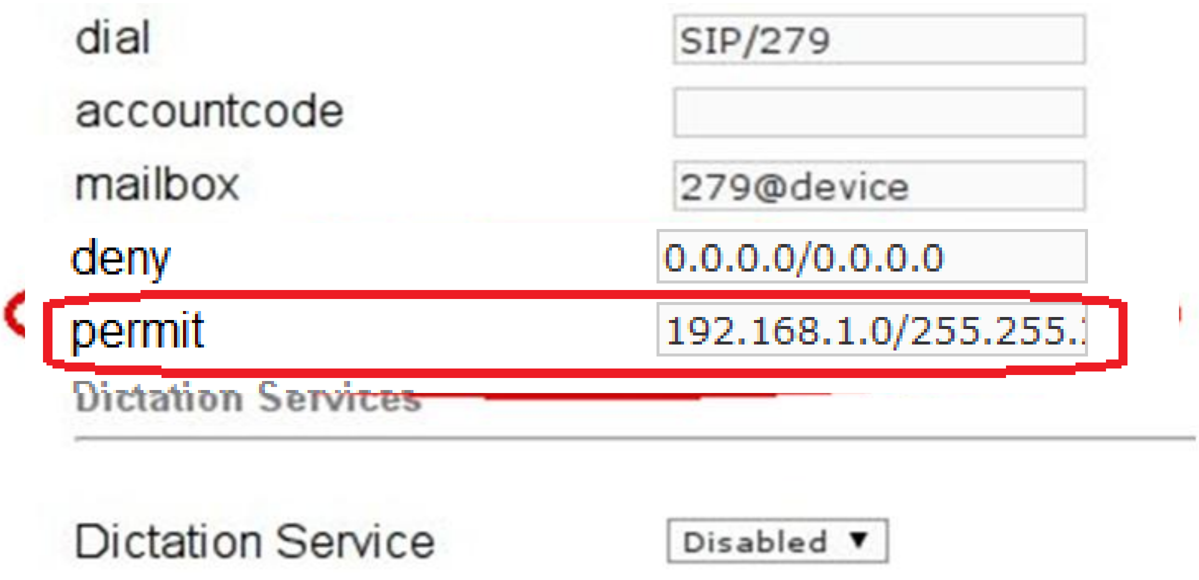
Telco Depot

How to Secure your TD system

Follow these simple steps to increase the security level of your system

1. Change your Linux root password from its default 'akuo-kfo' to a unique complex password that you will remember and make sure never to lose as this password is NOT recoverable.
    a. To do so simply connect a keyboard and monitor to the system.
    b. login as 'root' and use the 'akuo-kfo' pasword.
    c. Invoke the *passwd* command and set a new password to the system. Note 'passwd' is NOT misspelled, this is the command.
2. Now we will restrict the registration of all internal extensions.
    a. log in to the TD system using your browser.
    b. click on the PBX tab. You should get the extensions view.
    c. For each of your LOCAL extensions add the following data as shown below. This will insure that no one can register this extension from outside of your local network. The data should be 192.168.1.0/255.255.255.0



dial	SIP/279
accountcode	
mailbox	279@device
deny	0.0.0.0/0.0.0.0
permit	192.168.1.0/255.255.:

Dictation Services

Dictation Service	Disabled ▼

3. Install "fail2ban" on your system. Fail2ban is a utility that scans log files (asterisk log file in our case) and searches for predefined log entries. Since attackers will try to register an extension and since they don't have the password for that extension, a log entry will be generated for each failed attempt. In this case "fail2ban" will pick it up and will restrict ANY further communication from that IP for the amount of time that is set in the configuration file. Follow these steps to install "fail2ban" on your system.
   a. connect a keyboard and monitor to the system and log in as root.
   b. invoke the following commands
      i. *yum install fail2ban*
      ii. *yum install python iptables*
      iii. *nano /etc/fail2ban/filter.d/asterisk.conf* - this will open a simple text editor. Simply copy and paste the following text. when done press the Ctrl X to exit and save

```
# /etc/fail2ban/filter.d/asterisk.conf
# Fail2Ban configuration file
#
#
# $Revision: 250 $
#

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# common.local
#before = common.conf


[Definition]

#_daemon = asterisk

# Option:  failregex
# Notes.:  regex to match the password failures messages in the logfile. The
#          host must be matched by a group named "host". The tag "<HOST>" can
#          be used for standard IP/hostname matching and is only an alias for
#          (?:::f{4,6}:)?(?P<host>\S+)
# Values:  TEXT
#

failregex = NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Wrong password
            NOTICE.* .*: Registration from '.*' failed for '<HOST>' - No matching peer found
            NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Username/auth name mismatch
            NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Device does not match ACL
            NOTICE.* .*: <HOST> failed to authenticate as '.*'$
            NOTICE.* .*: No registration for peer '.*' (from <HOST>)
            NOTICE.* .*: Host <HOST> failed MD5 authentication for '.*' (.*)
            NOTICE.* .*: Failed to authenticate user .*@<HOST>.*
# Option:  ignoreregex
# Notes.:  regex to ignore. If this regex matches, the line is ignored.
# Values:  TEXT
#
ignoreregex =
#
```

iv. *nano /etc/fail2ban/jail.conf* - we will now edit the jail file. Simply copy and paste the following text. when done press the Ctrl X to exit and save. make sure to change the parameters in RED if you want.

```
# /etc/fail2ban/jail.conf

[DEFAULT]
ignoreip = 127.0.0.1 192.168.1.0/24

[asterisk-iptables]
enabled  = true
filter   = asterisk
action   = iptables-allports[name=ASTERISK, protocol=all]
           sendmail-whois[name=ASTERISK, dest=you@company.com, sender=fail2ban@company.com]
logpath  = /var/log/asterisk/fail2ban
maxretry = 3  # this is the max tries someone can try registering an extension
bantime = 3600 # this is how long (in seconds) that IP will be ban if failed to register
```

v. *nano /etc/asterisk/logger.conf* - we will now edit the jail file. Simply copy and paste the following text. Make sure to insert this text at the TOP of the file. When done press the Ctrl X to exit and save.

```
[general]
dateformat=%F %T
[logfiles]
full => notice,warning,error,debug,verbose
fail2ban => notice
```

c. asterisk -rx "module reload logger"
d. chkconfig iptables on
e. chkconfig fail2ban on
f. /etc/init.d/iptables start
g. /etc/init.d/fail2ban start
h. Check if fail2ban started properly by invoking this command *iptables -L -v* You should see "fail2ban-ASTERISK" in the output.

If you have any issues implementing these protective measures, please do not hesitate to contact us 1-800-390-1200